

Generators of pseudorandom sequences are widely used objects, not in the least place because of their application in stream ciphers. One of the ways to improve resistance to different types of attack is to use compression on the generated sequence in order to remove redundant information, that might lead to an attack against the generator. In this work we try to explore from a wider perspective the theoretical foundations for compressing pseudorandom sequences created thus far. Using this general view we will examine some known attacks against the PRN generators and look for a way to resist such attacks.